Stop Spreading the Data

PSM, Trust and Third-Party Services

Sørensen, Jannick Kirk; van den Bulck, Hilde; Kosta, Sokol

Published in:
Journal of Information Policy

DOI (link to publication from Publisher):
10.5325/jinfopoli.10.2020.0474
10.5325/JINFOPOLI.10.2020.0474

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

STOP SPREADING THE DATA

PSM, Trust, and Third-Party Services

Jannick Kirk Sørensen, Hilde Van den Bulck, and Sokol Kosta

ABSTRACT

The article analyzes problems relating to public service media use of third-party services that track, collect, and analyze user behavior. The article extends a rights-based conception of privacy to privacy as a social phenomenon based in trust, relevant to public service media as "islands of trust." However, data of European public and private media sites show that public service media, especially those that run advertising, show few differences with private media in their use of third-party services. The European Union's (EU's) General Data Protection Regulation (GDPR) did significantly change this, suggesting a need for public service media to prioritize ethical values over market considerations.

Keywords: third-party web services, trackers, rights-based approach, information privacy, trust, public service media, private media

Expanding on a rights-based approach, we analyze problems relating to legacy, in particular public service, media use of third-party services that track, collect, and analyze user behavior through the lens of privacy-as-trust. Theoretically, the article extends a rights-based conception of information privacy to a conception of privacy as a social phenomenon based in trust and how this is particularly relevant for public service media as "islands of trust" in an era of datafication and surveillance. However, empirical data of a sample of European public and private media sites show that public service media, especially those allowed to run advertising, show limited differences with private media in their use of third-party services. The observation that European Union's (EU's) General Data Protection Regulation (GDPR) as a legal instrument has not had a significant impact on the number of third-party services suggests some

Jannick Kirk Sørensen: Aalborg University of Copenhagen
Hilde Van den Bulck: Drexel University
Sokol Kosta: Aalborg University of Copenhagen
DOI: 10.5325/jinfopoli.10.2020.0474

limitations when thinking of privacy from a purely legal perspective on communication rights and helps to emphasize the need for public service media as duty-bearers to prioritize ethical values, in particular trust, over market considerations to maintain their trusted relationship with citizens.

This contribution expands on a rights-based approach to information privacy and autonomy through the concept of privacy-as-trust and its relationship to users' (rights holders') trust in (public service) media (duty-bearers). This serves as a framework to analyze the use of third-party services—that, potentially, track, collect, and analyze user behavior[1]—in a sample of European public and private media. We analyze and discuss longitudinal data from a wide-ranging sample of European public service media (hereafter: PSM) and private media. Findings are used to discuss how respect for citizens' trust, more than a legal obligation, needs to be at the heart of a privacy policy of PSM to ensure their continued position as trusted institutions.

The exponential growth of web-based media services, such as social media, as well as the logic of optimizing audience for user loyalty and advertising efficiency nudge legacy media, like newspapers and broadcasters, to implement new technologies. Technological innovations provide legacy media with new opportunities for content creation and dissemination and for audience relations. For instance, to help their Internet-based content reach increasingly diversified audiences, media track users' behavior, often in collaboration with outside web services. So, when a user loads a webpage, a number of external services are contacted, triggered by embedded scripts and cookies. These third parties can perform a range of services: some deliver or help distribute audio/video streaming; others provide technical resources like computer code to build webpages, or help editors, marketing people, media researchers, and managers to analyze user behavior; other third parties show content from social media or advertising. As such, legacy media have become part of a datafication process in which online human action (clicks, likes . . .) is tracked and translated into quantified and quantifiable "big data."[22] We focus on third-party servers that track, collect, and analyze user behavior to report site activity to editors or to optimize exposure to content and advertising.

These audience data are not just functional but also tradable and, thus, a potential source of revenue that can counter legacy media's loss of advertising.[33] However, they come with a set of legal and ethical issues relating

1. Roesner, Kohno, and Wetherall.
2. Mayer-Schoenberger and Cukier; Van Dijck.
3. For example, Donders et al.; Raats, Evens, and Pauwels.

to infringement of citizens' rights, leading to discussions about privacy and surveillance.[4] This concerns all media but especially PSM, given their role and position as trusted institutions.[5] Law and policymakers try to deal with these issues from their end. The most formidable reaction to date has been the EU's legal framework: the so-called GDPR.[6] In force since May 25, 2019, the GDPR aims to give users more control over the collection and distribution of their personal information. The main aim of this article is not the evaluation of (the impact of) the GDPR. However, we analyze long-term data to answer the research questions: *Since the introduction of the GDPR, do audiences from legacy media, especially PSM, meet fewer third-party servers when accessing their digital offerings than before GDPR and does this differ between media that can/do and can/do not carry advertising*?

The principle goal of this contribution, however, is to understand whether the role of PSM as trusted institutions impacts their use of trackers, that is, if the values associated with PSM have an impact on the technical solutions they employ in their daily operations. Since tracking and data mining can occur without users' knowledge, infringing their privacy is a real threat and legacy media's respect for their audience's privacy becomes a crucial ethical issue, beyond user consent. We argue that respect for privacy and disclosure revolves around trust, following Waldman's[7] notion of privacy-as-trust: trust as a social phenomenon where the rights holders (users) trust the duty-bearers (media) to do the right thing after consenting to let them use their data. This is of particular relevance to PSM as their brand identity and reputation—and, thus, their public financing—are based in their role and position as trusted institutions. For interactive digital platforms, the burden of demonstrating integrity and independence falls back on the media organizations, in terms of ensuring that their users and their browsing behavior cannot be identified by external, third-party services. Especially in the context of exploitation of these data for commercial revenue, *the question is whether PSM more than private legacy media are vigilant in their use of third-party services, whether this differs depending on whether they can/do carry advertising and whether GDPR has worked as a wake-up call in this regard.*

4. Srnicek; Zuboff, The Age of Surveillance Capitalism.

5. In full: Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. For full text, see https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

6. Ibid.

7. Waldman.

To study these questions, after this introduction, we develop a theoretical framework that starts from a rights-based approach and combines the complementary theoretical perspectives of media values, media and information law, and policy and computer ethics to understand privacy-as-trust in relationship to PSM as "islands of trust" in a context of datafication and, ultimately, surveillance capitalism.

This theoretical framework serves as a background to our data analysis. Data were collected through extensive and repeated tracking of third-party activity on media-related websites. From a dataset of +61.5 million recordings of HTTP responses for +12,000 web pages from 1,291 websites visited 44 times spanning before and after the commencement of GDPR (nine times before May 25, 2018), we selected 342 media websites from 39 European countries (#107 from European Broadcasting Union [EBU] members, #235 from private media). Data were analyzed and third-party servers identified and categorized into 16 categories, including Advertising, Analytics, Distribution technologies, and Malicious servers (see method section).

The result section looks at various characteristics of third-party services before focusing on differences between private and public media, changes over time, especially before and after GDPR, and country specific differences. These results are discussed in light of the ethical implications of what may legally be a licensed use of audiences' data by third-party services. We assumed that the more third-party servers involved in a webpage visit, (1) the higher the potential exposure of personal, identifiable information and, thus, (2) the more the ethical aspects of privacy and, ultimately (3) the value of trust—crucial to the working of media, especially PSM—are compromised. Finally, we evaluate whether and how, in an area of individual rights infringement, media policies that work from a rights-based approach should move beyond legal instruments such as GDPR to an understanding of privacy-as-trust.

Theoretical Framework: Communication Rights, Privacy-as-Trust, and PSM

A Rights-Based Approach and Privacy: From the Legal . . .

This contribution builds a framework for analysis of third-party services by European legacy media, especially PSM, through an expanded rights-based perspective. Such a framework takes Human Rights as a guiding principle and aims to identify rights-holders and duty-bearers as it "seeks

to strengthen the capacities of rights-holders to make their claims and of duty-bearers to satisfy those claims."[8] In policymaking regarding third-party service data transfer, this perspective requires policy initiatives to start from the communication rights of media users (the rights holders) and to ensure the responsibilities of the media companies (the duty-bearers) in realizing those rights with a policy aim to help redress the disturbed balance between the two parties involved.

Among the key communication rights, identified by Nieminen,[9] are privacy and citizens' autonomy in deciding what happens to their personal data, next to access, availability, competence, and dialogue. In the context of third-party services, privacy certainly has received considerable attention from law and policymakers, looking to protect personal data and privacy in general and to enforce duty-bearers' responsibilities. National law and policymakers, however, are hampered in their response because of the dominance of neo-liberal and free speech paradigms,[10] difficulties in grasping the technologically complex details involved[11] and, most of all, limited options to tackle global companies that escape national control.[12] As such, national policymakers have struggled to address structural causes and barriers to citizens fully performing their communication right to privacy and autonomy.[13] Instead, as part of its wider policy attention to citizen's privacy, the EU has taken the lead, defining requirements for providers of interactive services regarding personal data protection and obtaining user consent about data collection.[14] Especially the EU's GDPR, in force since May 25, 2018, provides extended rights to users to protect personal information, including the right to be informed about the processing of personal data, and the right-to-be-forgotten, that is, have all personal data removed from the provider's records.

. . . to the Ethical

However, collecting user data involves more fundamental ethical questions as data collection can be lawful but at odds with ethical principles of good

8. Nyamu-Musembi and Cornwall.
9. Nieminen.
10. Van Dijck.
11. Van den Bulck et al.
12. Vaidhyanathan.
13. Boesen and Martin.
14. EU Parliament; European Commission.

behavior toward end users, that is, rights holders. According to Shoshana Zuboff,[15] tech companies are the nodal points of surveillance capitalism that exploits human behavior (user data) as raw material and refines it into prediction products that can be sold to interested parties including advertisers. To get more data, more precise data, and more heterogenous data, surveillance capitalism actively stimulates users to produce more data via different types of devices and sensors. To individual users, this may not feel as a big threat as they conveniently use the platforms' services. For Zuboff, privacy is not so much eroded as it is redistributed. A user's right to decide over their privacy, for example, via privacy policies, has been transferred to the locus of surveillance capitalism. If you want to use the service, you must accept terms and conditions. Thus, the problem is not the violation of individual users' specific privacy but the ethics of those who hold "instrumentarian power" (21–41).

A key question concerns who exactly is expected to be ethical: Is it restricted to third-party services or does it extend to the media that use them? Recent discussions revolve around the ethical role of tech and social media giants such as Facebook. A good illustration is the 2019 Federal Trade Commission (FTC) fine of $5 billion for Facebook's violation of various privacy rules. The highest fine in FTC's history, the number is dwarfed by Facebook's $15 billion revenue in the Spring quarter of 2019 and its $22 billion profit in 2018. In a cynical turn of events, the fine resulted in Facebook's stock prices going up.[16] This relative inability and often reluctance to regulate and curb tech and social media giants, has resulted in law and policymakers appealing to these companies' ethical awareness. As Wagner[17] suggests, though, in this context, "ethics" is the new "industry self-regulation" (1) with government regulation considered as part of the problem rather than the solution and tech and social media giants turning to ethics as a catch-all phrase and a means to be seen to be doing it.

Far less discussed is the ethical behavior of legacy media, both private and PSM. We focus on PSM that have a history of being called upon to act ethically as so-called "islands of trust." This has two complementary theoretical perspectives—PSM values and computer ethics—that come together in Waldman's[18] notion of privacy-as-trust.

15. Zuboff, "We Make Them Dance."
16. Patel.
17. Wagner.
18. Waldman.

Trust in Media and the PSM Conundrum

While ethics in relationship to PSM covers many issues, it crucially revolves around the notion of PSM as trusted institutions.[19] "Trust" can be understood as "the willingness of a trustor to be vulnerable to the actions of a trustee based on the expectation that the trustee will perform a particular action, irrespective of the ability to monitor or control that other party"[20]: that is, PSM as a place of trust, a space that people turn to assuming it has their best interests at heart. Indeed, in return for public funding and a continued position in a competitive market, governments stipulate and societies expect a commitment to ensure universality, contribute to identity and social cohesion, and provide a mix of information, inspiration, and entertainment, while maintaining high standards of quality, decency, and objectivity, resulting in high levels of trustworthiness.[21] Trust was always an intrinsic but implicit value for PSM. From the 1990s onward, it became an explicit topic in discussions regarding the legitimacy and relevance of PSM institutions amid fierce commercial competition and "hostile" government scrutiny. This coincided with people's trust in legacy media in general showing a slow but steady decline[22] to the point where it can no longer be taken for granted. This results from a range of trends including tabloidization, personalization, and developments such as the upsurge in dis- and misinformation.[23] Infringement of the communication right to privacy and disrespect for the autonomy of users in decision-making regarding the use of their personal data can further undermine this trust.

In an increasingly commercial and self-serving ecosystem, PSM, so far, have stood out as "islands of trust," a descriptor coined by the Digital Strategy Group[24] of the EBU's.[25] Biltereyst[26] calls it the "aura of trust" that "includes a feeling of quality, reliability, honesty, competence and good intentions" (341). Research confirms that in countries with strong PSM, trust in radio and television broadcasting is stronger.[27]

19. Curran; Carey.
20. Mayer, Davis, and Schoorman.
21. Van den Bulck; Born and Prosser.
22. Hanitzsch, Van Dalen, and Steindl; For example, Jones; Stoll.
23. McChesney and Nichols; Allcott and Gentzkow; Tsfati and Ariely.
24. EBU Digital Strategy Group.
25. PSM institutions representative and lobby organization; Bardoel and d'Haenens.
26. Biltereyst.
27. EBU Media Intelligence Service; EBU.

However, neither conceptual thinking nor empirical measuring of trust in relationship to PSM relates to the issues at hand as they are rooted in predigital standards regarding content and conduct, rather than to privacy problems that result from the datafication of legacy media. To remain relevant,[28][28] PSM institutions have a vested interest (and most often a mandate) to keep up with and invest in digital developments, including the use of third-party services, be it within the confines of legal frameworks such as the GDPR. However, for PSM institutions to do so in a way that it does not undermine their unique position as trusted institutions and that they remain loyal to their core values,[29] they must think beyond their traditional understanding of trust as well as the confines of a purely legal approach. This is especially the case for PSM that are allowed to generate part of the revenue from commercial sources, given the abovementioned trade in data.

Privacy-as-Trust

Where "trust" in the context of PSM traditionally refers to quality standards in content and conduct, in computer science and computer engineering literature, trust typically is discussed along with "security" and "privacy": Trust is seen as prerequisite for security in personal data exchange between system components or systems: Can the receiving subsystem be trusted? Can the received data be trusted? Trust is a matter of formalized software design procedures and structures—trust models.[30] In an early contribution to computer engineering, Denning[31] defines trust as "an assessment that a person, organization, or object can be counted on to perform according to a given set of standards" (37). It is not an inherent property of a system (or person, or organization) but a contextual assessment made by an observer, always subject to reassessment. Denning believes that market forces, over time, will ensure the provision of trusted software solutions, as "the value of a person, organization, or object in the market will be determined to a large part by the amount of trust that others have in them" (38). Furthermore, trust is gained over time, not by formal certificates: "If a software product shows no evidence of containing malicious code after

28. Bardoel and Lowe.
29. Van den Bulck Hilde and Moe; Just and Latzer.
30. Chokhani.
31. Denning.

several years of use, then it will be trusted to be non-malicious regardless of whether that property was formally proved" (38). More recently, the field has developed different types of "trust models,"[32] including a so-called "zero trust model."[33]

Computer science's instrumental understanding of trust shows its importance to secure system operations and confidentiality of the data processed. In relationship to PSM organizations, this conception needs to be extended to a human relation between a user and the service provider (i.e., PSM). Waldman,[34] working from a legal perspective, incorporates this in his concept of privacy-as-trust. For him, "[privacy] is, at its core, about the social relationships governing disclosure between and among individuals and between users and the platforms that collect, analyze and manipulate their information for some purpose" (3). He argues that this goes beyond the "notice and choice" approach (8) that is typical of consent buttons as "it gives users little to no help when making disclosure decisions, and it offers even less protection when Internet companies use our data in unexpected and invasive ways" (8), especially in a context of algorithms and Artificial Intelligence. Because rights holders share when they trust, it is important to consider information privacy as a social norm based in trust: they expect "disclosure to occur in safe environments buttressed by concurrent norms of confidentiality and discretion" (8). Consistent breaches of confidentiality and discretion undermine users' trust in the institution. For PSM institutions, respecting privacy of its users' data beyond notice and choice becomes a matter of "protecting relationships of trust" (88), also in their collaboration with third parties involved in data collection and handling.

Research into Third-Party Servers

The activity of third-party servers has caught the interest of privacy-concerned researchers, typically working from a quantitative—technical research perspective.[35] Some authors[36] focus on the technologies that identify users in the browser from one website visit to the next, either through

32. Yan.
33. Ahmed et al.; Tao, Lei, and Ruxiang; Gilman and Barth.
34. Waldman.
35. Urban et al., "Towards Understanding Privacy Implications."
36. Falahrastegar et al.; Wambach and Bräunlich.

"cookies"[37] or through so-called "finger-printing" technologies that identify users across devices without cookies.[38] Other studies map and categorize which third-party sites are contacted when users visit webpages. For instance, using automatic scripts, Englehardt and Narayanan[39] analyzed the one million most popular websites in the world in 2016. Visiting the pages 90 million times in one month, they found 81.000 different third-party URLs, yet only 123 were present at more than 1 percent of the websites indicating a "long tail" distribution of third-party URLs. Their study further showed that news websites have the highest average number of third-party URLs, while government, nonprofit and university organizations' websites have the lowest number. Urban et al.[40] show that the sharing of data in advertising networks declined at the start of the GDPR but afterward showed a slight rebound. The amount of tracking was not affected. Before that, Urban et al.[41] found that the GDPR appeared to have an effect on the illegal but wide-spread praxis of "cookie synchronization" whereby uses can be identified across websites and be subject to "re-targeting" advertising, that is, advertising that reminds you of your browsing history. Urban et al.[42] further investigated the tracking capabilities and related privacy implications of adware. Analyzing developments in third party presence in the period February to September 2018 for eleven types of websites published either by private or public organizations, the authors[43] find large differences among the different categories of websites. A study[44] comparing unique URLs found on PSM and commercial broadcast media's web pages during six visits between December 2016 and August 2017, that is, before the GDPR, showed an average of 42.95 third-party URLs among private media compared to 70.42 for PSM with advertisements, 37.60 for PSM with possibility for advertisements, and 17.33 for PSM not allowed to display commercial advertisements. While low numbers of third-party URLs for PSM could be related to a ban on commercial advertisements, private media, too, showed considerable variation with a span between eight and 88 unique third-party servers. The current study wants to find

37. Internet Engineering Task Force.
38. Acar et al.
39. Englehardt and Narayanan.
40. Urban et al., "Measuring the Impact of the GDPR on Data Sharing."
41. Urban et al., "The Unwanted Sharing Economy."
42. Urban et al., "Towards Understanding Privacy Implications."
43. Sørensen and Kosta.
44. Sørensen and Van den Bulck.

out (1) if these comparisons between private and public service broadcast media hold and (2) whether the GDPR has affected the presence of third-party servers.

Other studies have focused on understanding the ownership and type of these third-party servers and the media's dependence on these. Lindskow[45] mapped the business network of 41 US media publishers and finds 1,356 business partners involved in building web pages for users, concluding that traditional news media webpage production involves a huge network of interacting companies. Sjøvaag et al.'s[46] analysis of the use of third-party services by news apps of legacy media suggests a divergent yet wide range of services as well as an increase in extent and complexity of the network over time but also shows that behind this wide variety of services are a smaller group of dominant players, such as Alphabet.

Methodological Set-Up

Data Collection, Cleaning, and Analysis

We sampled websites from two categories: websites published by PSM organizations and by legacy private mass media, for example, newspapers and commercial broadcasters. As a working definition for PSM, we use the criterion of membership of the EBU,[47] while the selection of private media sites was based on Reuter's Institute Digital News Report 2017.[48] For the 22 European countries featured in the Digital News Report, we selected the top five most popular news sites in terms of percentage weekly, for the remaining 17 countries, we used Alexa web service, selecting top news sites for the specific countries.[49] This way we found 235 private media sites and 107 websites from EBU members. Using data provided by the EBU on the advertising status for EBU members, as well as our own investigations, we further categorize sites from EBU members in three groups, reflective of their relationship to commercial advertising: 56 EBU member sites allow or feature advertising while it is forbidden at 38 websites. For 13 EBU member websites, the situation is unclear; in the following, they are labeled

45. Lindskow.
46. Sjøvaag et al.
47. https://www.ebu.ch/about/members.
48. Newman et al.
49. https://www.alexa.com.

"Advertising not seen." We assume that all private media in our sample are allowed by national or EU regulation to have commercial advertising.

To simulate a user's browsing behavior, we visited from an IP-address in the EU 10 web pages from each website. To ensure comparability across the sample dates, we visited the same set of webpages throughout the entire sampling period. The sampling period spans 20 months from February 2018 to October 2019 and counts 44 visits/sampling dates, nine of which took place before the commencement of GDPR on May 25, 2018.

Visiting the pages was by means of an automated procedure that simulates human browsing behavior. On a virtual machine placed within the EU, we used an open-source python/selenium script[50] to load the webpages in our browser (Mozilla Firefox), to scroll it and to record all HTTP-request, -responses, and -redirects. In this way, we recorded all interactions a user's browser has with third-party servers (hereafter: "TPs") as well as with the server of the media website being visited (the "first-party server"). All web pages were accessed from the same browser and the IP-address from the EU. The cookies set during browsing were preserved between each visit. The browser had no other cookies or other user-profile information that would advance the identification of the user and his interests for example, for the sale of advertising, re-targeting and the like. The browser never made a login to any social media or Google, thus representing a disinterested user with no shopping behavior and no social media activities. In all cases, the browser ignored "GDPR Consent" dialogue boxes; our findings thus represent an ignorant, passive user that does not explicitly allows transfer of person data or interaction with TP servers, a procedure that the EU High Court has ruled illegal October 2019 in the so-called Planet 49 case.[51] Here the Court ruled that an active consent—for example, via a click in "check-box"—must be given by the user. Assuming that the user consents to a site's privacy policies by the continued visiting of the website does not provide sufficient legal basis for fulfilment of the GDPR. In this sense, all visited websites included in our sample violated the GDPR as they reacted to our requests.

We based our analysis on the recording of all successful HTTP responses (status = 200) from the TP servers' URLs. From the total set of HTTP

50. We use the OpenWPM framework developed by Steven Englehardt and Arvind Narayanan, published as open source at https://github.com/citp/OpenWPM. See also: Englehardt and Narayanan.

51. EU Court case C-673/17. Accessed February 2, 2020. http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1447493.

responses (+50 million for our 44 visits), we identified for each visited site, the unique top-level TPs that appeared during the browsing of the 10 pages from the visited site. Subsequently, we categorized the TPs to identify the possible purpose of the TPs' interaction with the browser, as well as the company hosting the TPs. Using various methods of identification and categorization, we first entered the TP URL into a browser. In cases where we obtained a readable page, we analyzed this manually to look for keywords indicating the overall purpose of the TPs, for example, a real-time bidding platform for the sale of online advertising or a content delivery network. In cases where the browser showed an HTTP error message (e.g., 404 page not found, 403 forbidden, or 500 Internal Server Error) or where content appear to be "fake," we checked whether the TPs URL was listed at www.threatcrowd.org as a site suspected of malicious behavior. If that was not the case, the TPs was labeled unidentifiable. The total number of found TPs exceed 3,500 URLs, so we have not yet been able to identify all TPs.

Categorization was based on a system developed by the authors and validated in a previous study.[52] The category *Advertising* covers tracking, sell-side and demand-side servers, real-time bidding, user profiling, advertisement agencies, and Data Management Platforms. *Analytics* covers performance, user profiling, and monitoring. *Content* contains web page elements (not advertising) from TPs, for example, syndicated news stories, embedded YouTube-videos. *Cybersecurity* covers anti-ad-fraud and services to protect websites. *Distribution technology* covers content delivery networks and video streaming. *Editorial* covers tools for publishers. The *Malicious* category consists of TPs listed as such at the cybersecurity community www.threatcrowd.org. The *Plug-in* category covers services embedded at the visited pages, such as blogs. *Privacy* TP URLs cover cookie consent services and similar. *Programming* covers libraries and fonts used to render the page. *Publisher* are TPs owned by media organizations. *Retail* are TPs from product brands and services websites. The *Search engine* category as well as the *Social media* contains services with these specific purposes.

Methodological Caveats

The collection, processing, and interpretation of data on TP presence involves a number of steps and decisions that can influence the result. First, the dataset is "created" not "observed," as it records automated nonhuman

52. This categorization builds on Sørensen and Kosta.

visits to websites conducted by a "user" (a script on a virtual machine). This means the absence of human browsing behavior; the script has no shopping habits, no credit card, smart phone, smart TV, or social media account. In short our "user" provides no extra "data signals" to advertisers and other TP providers.[53] One implication of the absence of real user data signals could be a more complicated online bidding process for the programmatic advertising as the lack of user information may make it more difficult to find a buyer for the advertising space "inventory."[54] However, due to the nature of a bidding process, the outcome differs each time an ad should be sold. This influences also the involvement of TP services in the bidding. The size of our dataset provides us however with "safety in numbers" that emphasizes the significant patterns in TP appearances.

Second, the processing of the collected data offers similar problems. For one, the number of different TP URLs must be interpreted with care. The same TP company can be present through several server names, which can account for unidentifiable and technical TP servers. Furthermore, Englehardt and Narayanan[55] and Lindskow[56] show that the number of new TP servers decrease with additional visits. So, while we made sure to visit the sites repeatedly both before and after the GDPR, results are still influenced by the number of iterations. Furthermore, not all TPs are equally harmful in respect to the potential privacy violation caused by the collected data. A network of many TP services—for example, provided by Google—may better utilize collected data than a single TP service that does not exchange data with other services.

Third, our analysis shows that many TP servers are programmatic, that is, triggered by embedded scripts that depend on a user's browser history (cookies), device history (fingerprinting), location (geo-location), match with existing user-profile data; for example, from social networks, or wrapped scripts in scripts. Finally, our analysis is based on HTTP responses, that is, the data actually delivered to the user's computer. Another approach would be to analyze HTTP requests and HTTP redirects that would provide information about what the TPs ideally wanted in terms of data. With these technical details in mind, let us turn to the main results and how to interpret them in light of the research questions and theoretical framework.

53. Acar et al.
54. Busch.
55. Englehardt and Narayanan.
56. Lindskow.

Results

General Findings

In 44 visits to the 342 media websites, we found 3,511 unique TPs. At the 235 private media sites, we found the highest number of unique TPs, namely 3,213. At the 56 PSM sites that allow advertising, we found 802 unique TPs. For the 13 PSM sites where we did not see advertising, we found 255 unique TPs. Finally, at the 38 PSM sites where advertising is forbidden, we found 224 unique TPs (see Table 1). Some sites have many TPs, others very few, indicating considerable differences within the categories of media sites (see also Figures 10–12).

A few TPs are present many times at many sites, but most TPs only appear a few times and/or on few sites, corresponding to a so-called "long tail" (see Figure 1). The "tail" is shortest and steepest for PSM sites where advertising is forbidden, longest for PSM media with advertising and for private media. The advertising at media sites thus seems to have an impact on the number of unique TPs a user will meet.

As Table 2 shows, advertising-related TPs represent the largest group, after the category of yet unidentified TPs. Almost all sites (98.83 percent) have Analytics TPs and a large majority (93.48 percent) has Advertising TPs. Many sites also use TPs for Distribution (89.77 percent) and Programming (89.47 percent), as well as Search Engines (86.55 percent), and Social Media (84.21 percent). However, privacy-related TPs are found at less than half (41.81 percent) of all sites, while malicious TPs occurred at almost one third of sites (32.16 percent).

TABLE 1 Overview of Found TPs

	PSM Ads Forbidden (n = 38)	**PSM Ads Not Seen (n = 13)**	**PSM Ads Allowed (n = 56)**	**Private Media (n = 235)**
Number of unique TPs found	224	255	802	3,213
TPs present at more than 80 percent of sites	0	2	5	10
Minimum and Maximum numbers of unique TPs found at a site (all visits aggregated)	Min: 2 Max: 38	Min: 3 Max: 113	Min: 2 Max: 243	Min: 3 Max: 327

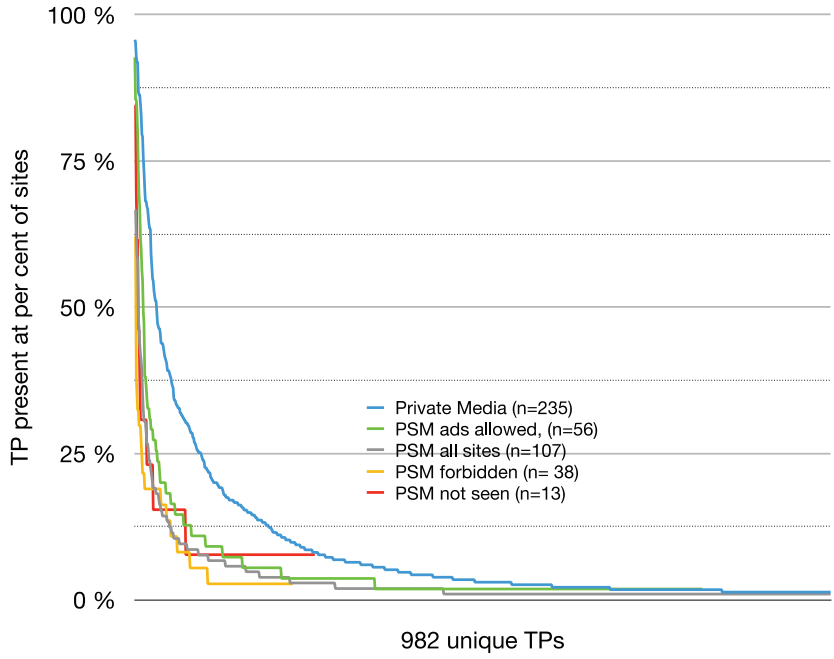

FIGURE 1 The long tails of TPs for different types of media.

TABLE 2 Distribution of TPs in Categories, All Media

TPs Category	Number of Unique TPs URLs	No. of Identified TP Companies	Number of Total Appearances	Average Number of Appearances Per Unique TP	Appearing at Percent of Sites (n = 342) (%)
Advertising	934	548	183,304	196.26	93.86
Analytics	131	77	49,822	380.32	98.83
Content	160	62	11,201	70.01	62.87
Cybersecurity	7	5	168	24.00	4.39
Distribution technology	187	94	38,532	206.05	89.77
Editorial	25	22	11,025	441.00	55.56
Malicious	42	13	2,293	54.60	32.16
Plug-in	29	25	3,362	115.93	35.96
Privacy	6	4	1,594	265.67	41.81
Programming	68	43	20,167	2,96.57	89.47
Publisher	253	73	13,963	55.19	52.92

TPs Category	Number of Unique TPs URLs	No. of Identified TP Companies	Number of Total Appearances	Average Number of Appearances Per Unique TP	Appearing at Percent of Sites (n = 342) (%)
Retail	95	43	3,180	33.47	46.78
Search engine	13	5	23,187	1,783.62	86.55
Social media	21	9	32,793	1,561.57	84.21
Unidentifiable	252	105	15,169	60.19	74.56
Unidentified	1,288	134	18,237	14.16	80.99

Comparing the number of unique TPs for each category to their total number of appearances, as presented in Table 3, reveals a high concentration of a limited number of TPs from just a few major companies in the categories of Search Engine and Social Media, while the advertising TPs, on average, have fewer appearances per TPs and originate from a wider range of companies. However, a more detailed look at the 548 Advertising-related TP companies shows a long tail headed by the dominant top 20 TP companies that account for 51.79 percent of all appearances, with a clear lead for Google. Importantly, though, the top has a number of company names less known by the general public, such as Criteo, RocketFuel, and AppNexus.

TABLE 3 Top-20 of Advertising-Related TP Companies

TP Advertising Company	No. of Appearances	Percent of All Appearances (n = 183304) (%)
Google	42,952	23.43
Company not identified	19,861	10.84
Criteo	7,013	3.83
RocketFuel	5,709	3.11
AppNexus	5,166	2.82
Adform	4,869	2.66
Rubicon Project	4,333	2.36
AOL	3,013	1.64
Smartadserver	2,705	1.48
Integral Ad Science	2,176	1.19
PubMatic	2,088	1.14
IPONWEB	2,032	1.11

(*Continued*)

TABLE 3 Top-20 of Advertising-Related TP Companies (*Continued*)

TP Advertising Company	No. of Appearances	Percent of All Appearances (n = 183304) (%)
OpenX	1,798	0.98
Casale Media	1,707	0.93
Taboola	1,698	0.93
Outbrain	1,588	0.87
adsrvr.org	1,576	0.86
Mediamind	1,530	0.83
Global Video Ads Group	1,506	0.82
AddThis	1,490	0.81
Total all identified companies	**23,091**	**51.79**

Table 4 shows each TP company's total percentage share of TP-appearances as it looks for private media sites and for the three types of PSM sites. The table is presented as a combined top 20 sorted descending after private media, then after EBU member with ads, then after EBU member no ads seen, and finally after EBU member ads forbidden. TP companies that are not among the top 20 for the specific type of media are marked in *italics text*. Percentage share is calculated for TPs from each TP company of all recorded unique TPs per site and visit (all visits aggregated).

For three types of media sites, namely private media and PSM media with advertising, TPs from Google had the biggest share of all TPs interactions in terms of unique TPs per site per visit.

Google's Dominance

Google TPs are more present at PSM sites with advertising than on private media site and PSM sites where advertising is not allowed. The share of all TP interactions for Google TPs varies between 14.7 percent (PSM—ads forbidden) and 27.9 percent (PSM—ads allowed), while Private Media have fewer unique interactions with Google TPs (21.5 percent). The large share can be attributed to Google's 32 different TPs. In Table 5, we present the Google TPs, their purposes and presence at media sites.[57] Google's

57. Private Media = 32 different TPs, EBU members with ads = 22 different TPs, EBU members advertising not seen = 14 different TPs, EBU members advertising forbidden = 15 different TPs.

TABLE 4 Top-20 of TP Companies for Four Types of Media Sites. Sorted After Private Media

TP Company	Private Media (n = 235) (%)	PSM Ads Allowed (n = 56) (%)	PSM No Ads Seen (n = 13) (%)	PSM Ads Forbidden (n = 38) (%)
Google	21.54	27.99	26.74	14.71
TPs—no company info	14.75 (1,860 unique TPs)	12.46 (271 unique TPs)	16.64 (63 unique TPs)	28.28 (83 unique TPs)
Facebook	4.93	6.29	5.74	4.55
Amazon	2.16	1.21	1.16	1.95
Twitter	2.10	2.71	3.62	3.60
Criteo	1.85	0.94	*0.08*	-
Chartbeat	1.54	1.36	0.90	3.60
Comscore	1.50	1.87	1.17	2.91
RocketFuel	1.41	1.13	0.92	-
AppNexus	1.31	0.75	*0.14*	-
Adform	1.22	0.67	*0.30*	*0.03*
Rubicon Project	1.09	0.83	*0.34*	-
Gemius	0.93	1.81	*0.62*	0.98
AOL	0.89	0.40	*0.25*	-
CloudFlare	0.74	0.90	1.00	0.89
JW Player	0.73	1.42	*0.80*	1.09
Smartadserver	0.69	0.41	-	*0.11*
AddThis	0.65	0.37	*0.32*	*0.61*
Moat	0.56	0.24	*0.28*	-
New Relic	0.55	2.32	2.31	1.48
NPO	-	1.99	2.14	-
Longtail Ad Solutions	*0.48*	1.19	*0.63*	*0.56*
Hotjar	*0.55*	1.17	-	0.70
AT Internet	*0.13*	1.01	2.33	6.37
Akamai Technologies	*0.51*	0.82	1.45	3.21
Cedexis	*0.13*	*0.34*	2.72	*0.15*
France Televisions	-	*0.26*	2.48	-
Microsoft	*0.18*	*0.17*	1.34	0.77

(*Continued*)

TABLE 4 Top-20 of TP Companies for Four Types of Media Sites. Sorted After Private Media (*Continued*)

TP Company	Private Media (n = 235) (%)	PSM Ads Allowed (n = 56) (%)	PSM No Ads Seen (n = 13) (%)	PSM Ads Forbidden (n = 38) (%)
Tealium	*0.18*	*0.17*	1.24	-
BootstrapCDN	*0.30*	*0.68*	1.24	*0.06*
jQuery	*0.32*	*0.57*	1.24	*0.31*
Qbrick	*0.20*	*0.51*	1.10	1.05
Nielsen	*0.25*	*0.37*	*0.18*	1.37
ReadSpeaker Holding	*0.003*	*0.09*	-	1.18
InSkin Media	*0.04*	*0.28*	-	0.92
Demdex	*0.27*	*0.42*	*0.72*	0.69

advertising service *doubleclick.net* was present at 225 out of 235 Private Media sites (= 95.74 percent), at 47 out of 56 PSM—ads allowed sites (83.93 percent), and at 11 out of 13 PSM—no ads seen (84.62 percent). Perhaps more interesting: *doubleclick.net* was found at seven out of 38 PSM ads forbidden sites. For *google-analytics.com*, a similar picture emerges, except that its share on PSM—ads forbidden' sites was higher (12 out of 38 sites, 31.58 percent).

Although Table 4 suggests Google's dominance, this must be qualified. Google dominated in three of four cases, but second in the ranking was a heterogenous group of TPs for which we could not identify the company behind. The long tail of TPs contributed with many interactions. For Private Media, 53 percent of all interactions were from TPs not in the top 20 while for PSM—ads allowed sites this was 42 percent; for PSM—ads not seen it was 39 percent; and for PSM—ads forbidden it amounted to 45 percent, suggesting a more differentiated picture. Analyzing the long tail for the 83 TPs without company info for PSM—ads forbidden, to a high degree they appear on German PSMs in the ARD group that are exchanging data with each other. In short, Google is important but definitely not the only important TP provider.

TABLE 5 The Presence of Google's 32 Different TP URLs at Four Different Types of Media Sites

TPs from Google	PSM ads forbidden		PSM ads not seen		PSM ads allowed		Private Media		TP purpose
	Sites (n = 38)	Percent (%)	Sites (n = 13)	Percent (%)	Sites (n = 56)	Percent (%)	Sites (n = 235)	Percent (%)	
Doubleclick.net	7	18.4	11	84.6	47	83.9	225	95.7	Advertising
google-analytics.com	12	31.6	11	84.6	47	83.9	218	92.8	Analytics
google.com	8	21.1	8	61.5	46	82.1	224	95.3	Search engine
googleapis.com	10	26.3	9	69.2	51	91.1	216	91.9	Programming
google.dk	4	10.5	4	30.8	38	67.9	216	91.9	Search engine
gstatic.com	5	13.2	4	30.8	40	71.4	199	84.7	Advertising
googlesyndication.com	1	2.6	2	15.4	34	60.7	204	86.8	Advertising
googletagservices.com	1	2.6	2	15.4	31	55.4	203	86.4	Advertising
googletagmanager.com	6	15.8	4	30.8	33	58.9	157	66.8	Advertising
ampproject.org	1	2.6			18	32.1	158	67.2	Programming
youtube.com	8	21.1	5	38.5	19	33.9	96	40.9	Distribution technology
ytimg.com	3	7.9	3	23.1	9	16.1	51	21.7	Content
googleadservices.com			3	23.1	3	5.4	59	25.1	Advertising
yimg.com					4	7.1	53	22.6	Content
appspot.com	3	7.9			5	8.9	47	2	Plug-in
gvt1.com					4	7.1	10	4.3	Malicious

(*Continued*)

TABLE 5 The Presence of Google's 32 Different TP URLs at Four Different Types of Media Sites (*Continued*)

TPs from Google	PSM ads forbidden		PSM ads not seen		PSM ads allowed		Private Media		TP purpose
	Sites (n = 38)	Percent (%)	Sites (n = 13)	Percent (%)	Sites (n = 56)	Percent (%)	Sites (n = 235)	Percent (%)	
1e100cdn.net	7	18.4	1	7.7	1	1.8	3	1.3	Distribution technology
googlevideo.com					1	1.8	9	3.8	Content
youtube-nocookie.com	1	2.6					2	0.9	Content
avads.net					1	1.8	2	0.9	Advertising
admob.com							3	1.3	Advertising
35.187.144.173.			1	7.7			2	0.9	Unidentifiable
codelab.is							2	0.9	Programming
google.de							2	0.9	Search engine
invitemedia.com					1	1.8	1	0.4	Advertising
cloudfunctions.net							1	0.4	Distribution technology
blogspot.com							1	0.4	Content
recaptcha.net							1	0.4	Programming
firebase.com					1	1.8			Programming
firebaseio.com					1	1.8			Programming
goo.gl							1	0.4	Search engine
kubnt.com							1	0.4	Unidentifiable

Developments Over 20 Months

Our overall sample spans a period of 20 months. Over this period, there was a significant decline in the average number of unique TPs per site for private media, concurrent with the enforcement of the GDPR in May 2018. For PSM sites, however, no significant decline is observed. The average number of unique TPs for PSM sites fluctuates over time but with no significant pattern except for a peak March 12, 2019, resulting from measurement problems (Figure 2).

The percentage distribution of TPs in different categories shows no dramatic changes over time, neither for Private Media (Figure 3) nor for PSM sites (Figures 4–6). Private Media and PSM sites with advertising allowed have a higher share of Advertising TPs than the two other types of PSM sites. The slightly growing number of unidentified TPs illustrates the dynamic nature of this kind of empirical research.

The relatively stable distribution of TPs categories can be compared to the growth in Google-related TPs. Figure 7 shows that the TPs from Google over the 20 months gain a bigger share of the total number of TPs interactions. Together, these data indicate that smaller TPs lose share to Google TPs. The biggest growth can be seen for PSM sites with advertising, a slightly smaller growth for private media, and just some growth for PSM sites where advertising is forbidden.

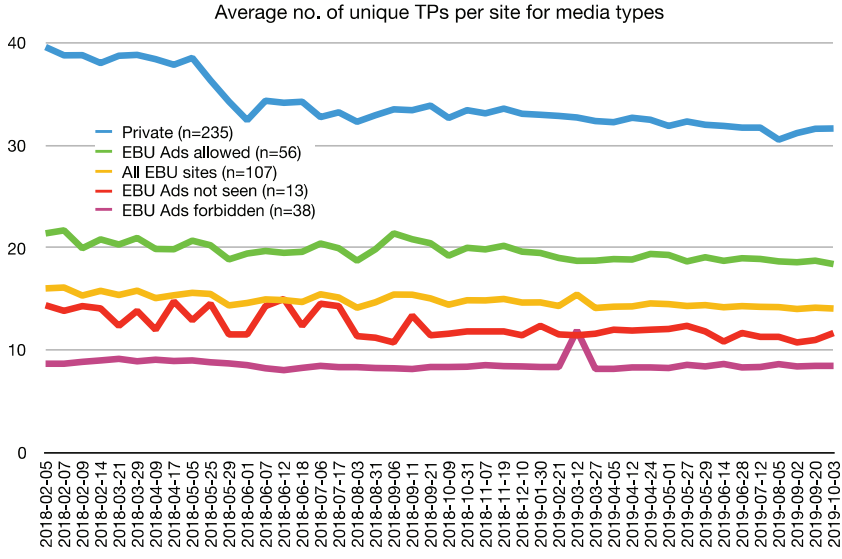

FIGURE 2 Developments in the average number of unique TPs per site for different types of media websites.

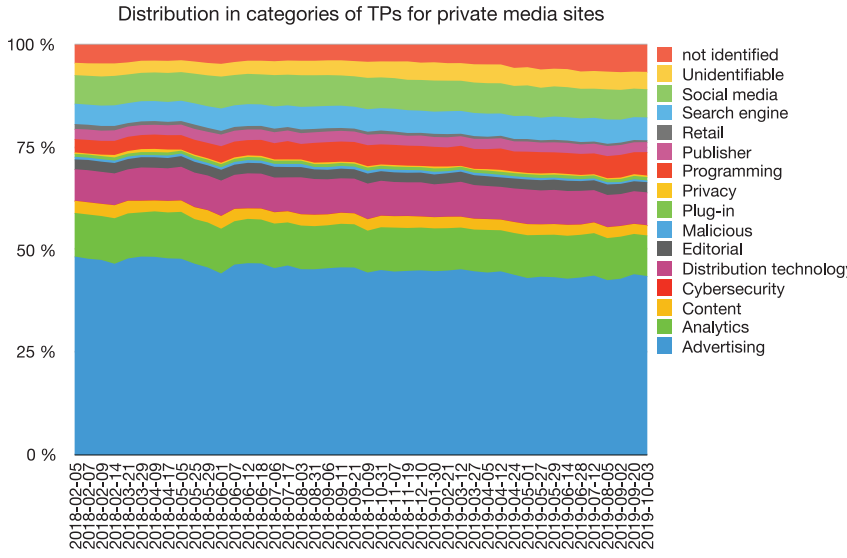

FIGURE 3 Distribution in categories of TPs for Private Media sites (n = 235).

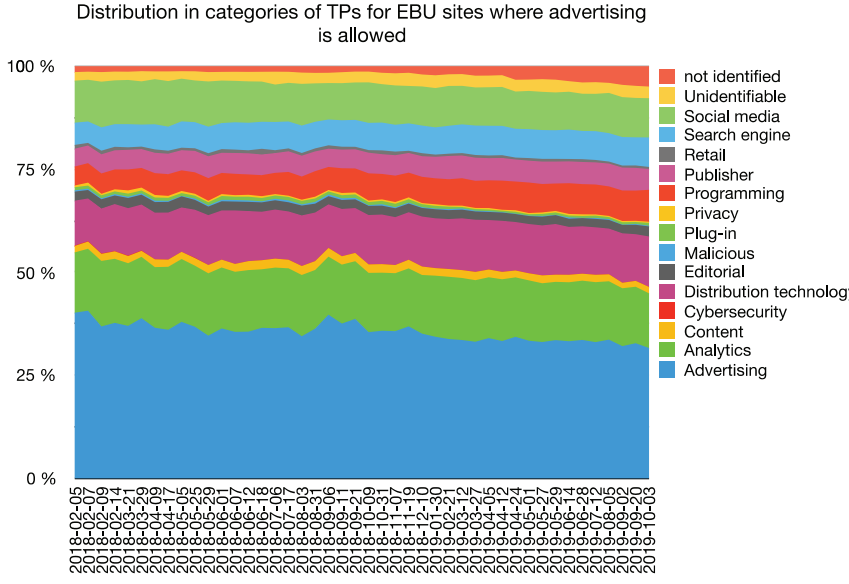

FIGURE 4 Average number of unique TPs in categories for PSM—ads allowed (n = 56).

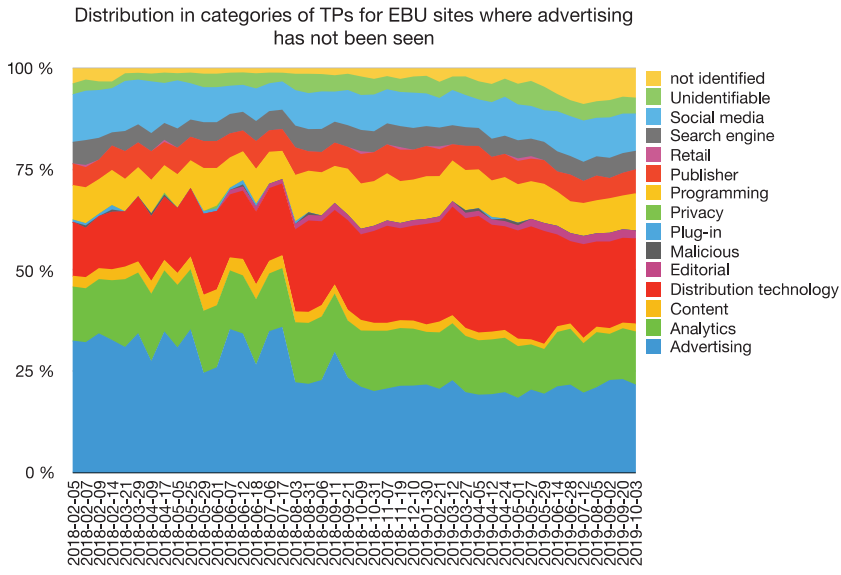

FIGURE 5 Distribution in categories of TPs for PSM—ads not observed (n = 11).

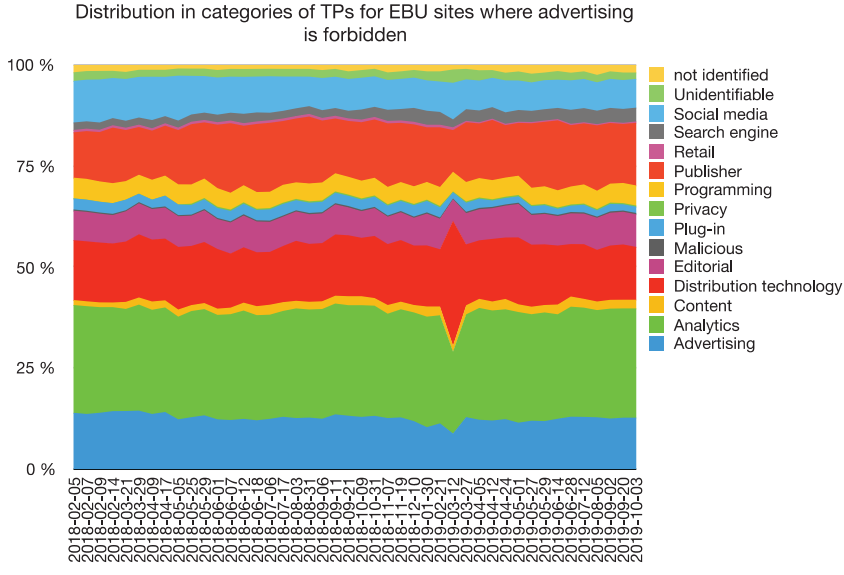

FIGURE 6 Distribution in categories of TPs for PSM—ads forbidden (n = 11).

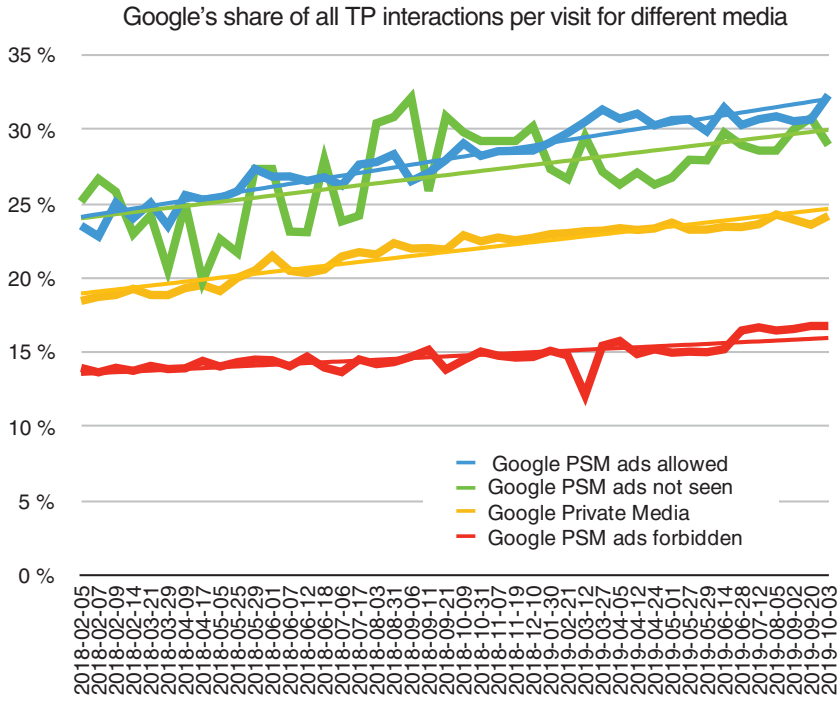

FIGURE 7 Google TPs growth over 20 months for four types of media with trend lines.

A Country Perspective

Comparative media analyses often are informed by categorization of countries belonging to different media systems such as those identified by Hallin and Mancini.[58] What is more, as legacy media systems to a high degree remain national or defined by language, a country-based analysis of our data could prove relevant. Figure 8 shows that PSM users in for example, Lithuania, Greece, Portugal, or Spain likely have been exposed to more TPs than PSM users in for example, North Macedonia, Cyprus, Ukraine, or Montenegro. For private media, a very different picture emerges. For instance, Figure 9 shows that a media user in Germany meets nine times as many unique TPs at private German media sites than at German PSM sites.

The ranked list of countries indicates a pattern that is very different from traditional categorization of national media systems. It calls for

58. Hallin and Mancini.

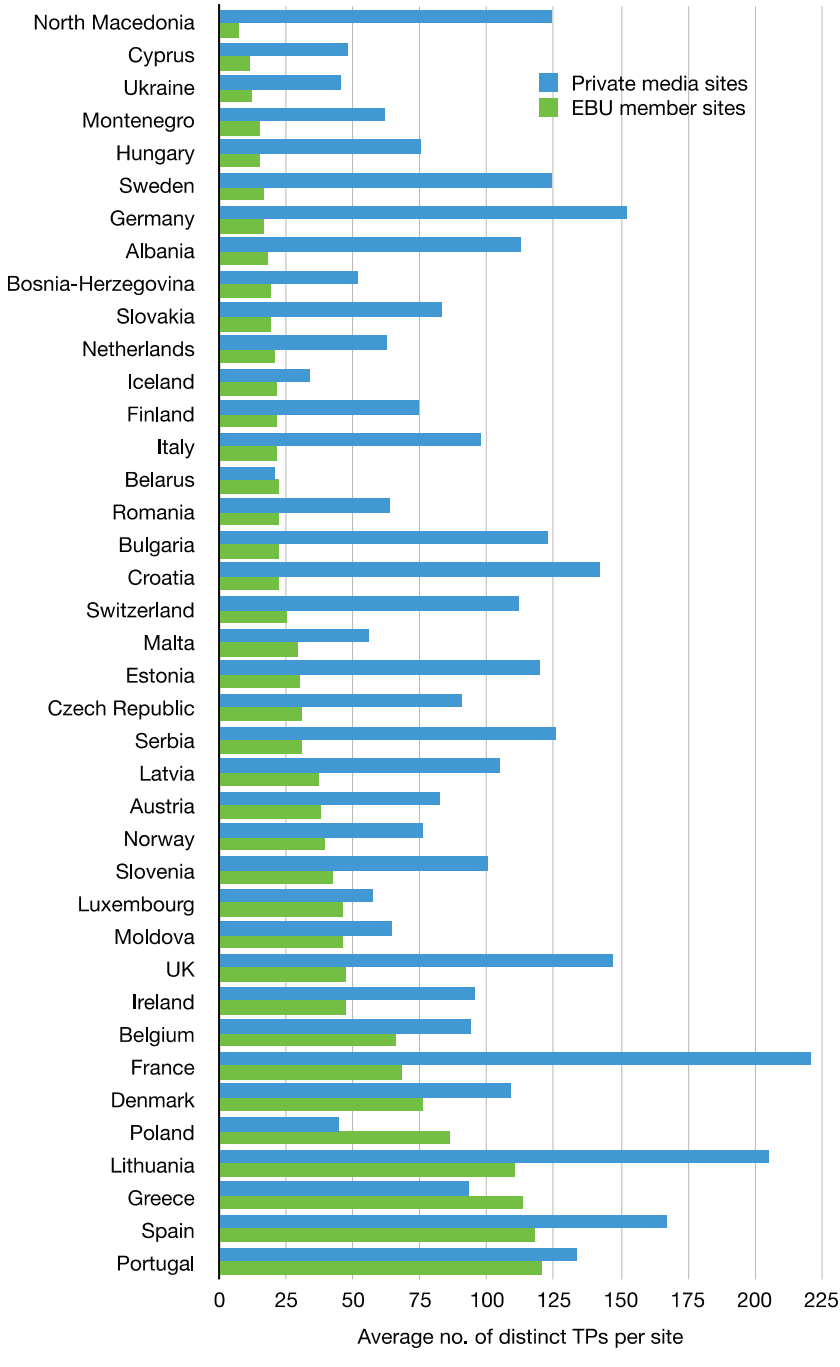

FIGURE 8 Country comparison—Average number of distinct TPs for Private Media sites and PSM sites, sorted ascending after PSM sites.

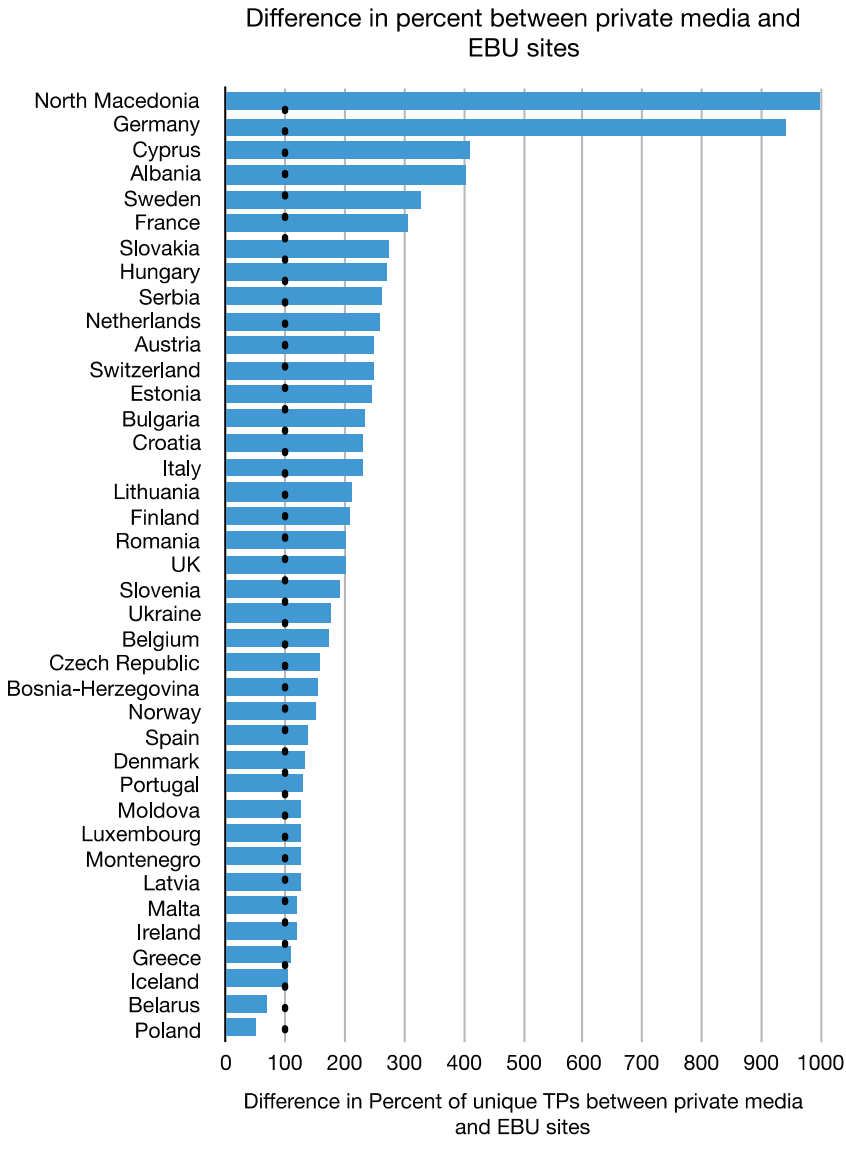

FIGURE 9 Ratio between average number of TPs for private media and PSM (all visits).

comparison with other dimensions of TPs interactions, for example, the different categories of TPs and the distribution between first-party and TP HTTP requests and responses. Finally, the list calls for an assessment of characteristics of the national media systems other than political (as in Hallin and Mancini), such as how technologically advanced individual websites are.

Developments for Individual Media

Taking a detailed look at the development for the individual PSM sites, a much more differentiated picture than that in Figure 2 appears. Figures 10 and 11 compare the first nine visits with the last nine with respect to number of unique TPs. On the x-axis, we see the change in percentage; on the y-axis, the average number of TPs of the first nine visits.

Sites with a decline in TPs typically had many TPs in the pre-GDPR visits and many of these sites allow advertising. The biggest decline (80.7 percent) was observed at the Austrian PSM orf.at. At the other end are sites with a growing number of TPs, many of which had relatively few TPs before May 25, 2018. However, 23 PSM sites[59] show growth of more than

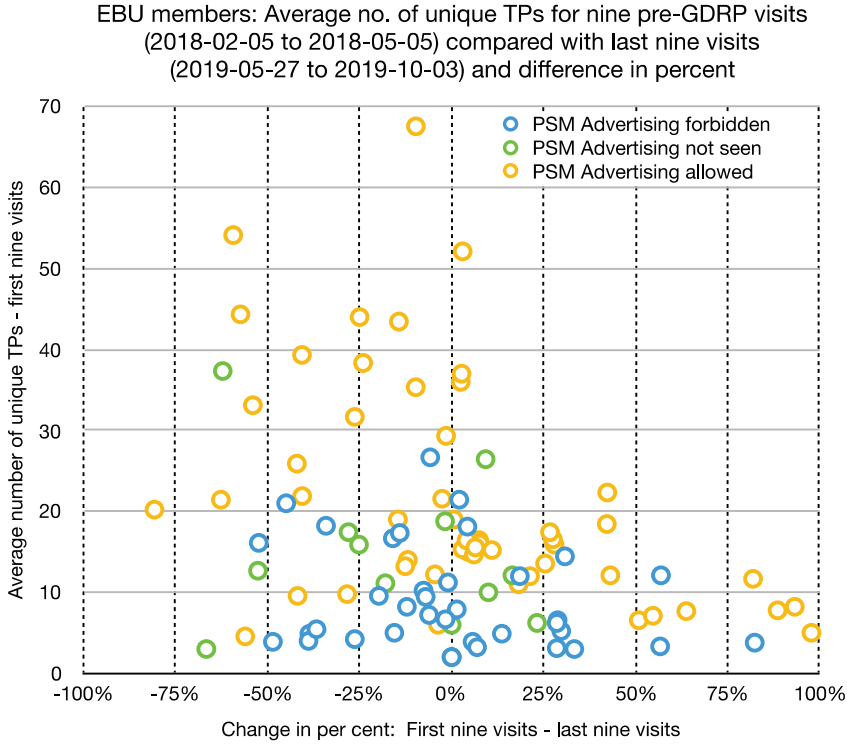

FIGURE 10 Development for number of TPSs in percent between first nine visits and last nine visits, focusing on PSM sites.

59. avrotros.nl, bhrt.ba, rtvslo.si, hessenschau.de, bnnvara.nl, vpro.nl, ruv.is, ndr.de, varagids.nl, eo.nl, bnr.bg, polskieradio.pl, lsm.lv, br.de, srf.ch, hr1.de, hr.de, hr3.de, kindernetz.de, dw.com, tg4.ie, tvm.com.mt, rainews.it.

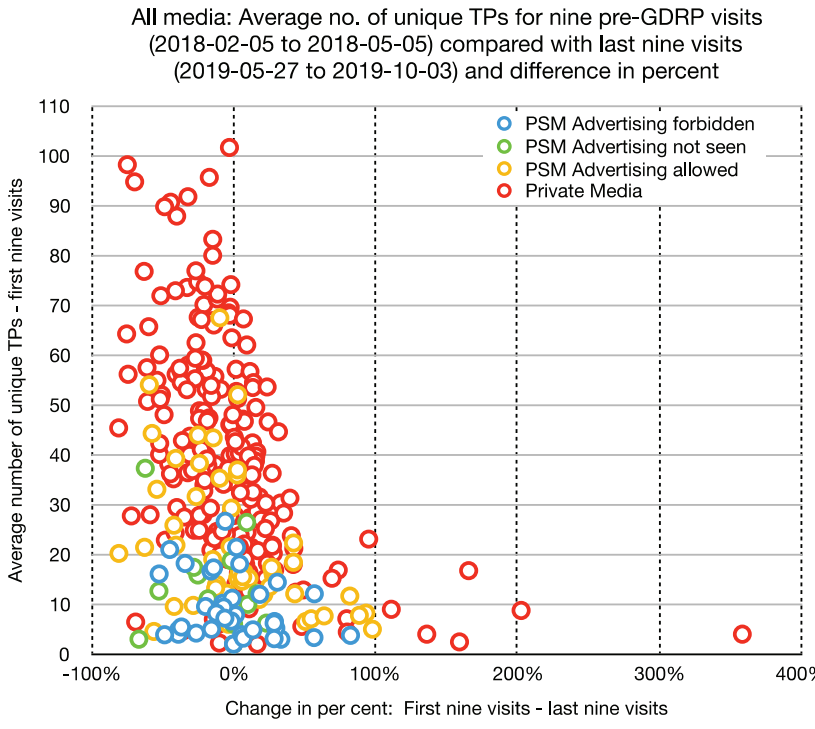

FIGURE 11 Development for number of TPSs in percent between first nine visits and last nine visits, including private media sites.

25 percent in unique TPs; 14 of these sites are PSM—ads allowed and the remaining nine are PSM—ads forbidden. Interestingly, in 13 of the 23 cases, the growth occurs on sites that had a low starting point with, on average, fewer than 10 unique TPs in the pre-GDPR visits. The other cases concern sites that already had more than average TPs pre-GDPR: The Polish PSM polskieradio.pl (22.33 TPs), the Latvian PSM lsm.lv (18.44 TPs), the Malta PSM tvm.com.mt (17.44 TPs), and Irish PSM tg4.ie (16.56 TPs).

In Figure 11, we add Private Media to the plot; the average numbers of unique TPs as well as the changes in number of unique TPs are more dramatic for Private Media. The number of unique TPs pre-GDPR for Private Media sites, overall, is at a higher level: 39.3 unique TPs on average in the nine pre-GDPR visits. The overall decline for TPs for Private Media is small at 3.0 percent. Again, some sites with a low number for TPs pre-GDPR showed a dramatic growth.

Regardless of media type, private and advertising funded PSM users seems to be exposed to many TPs. When we identify the unique TPs for

the entire sampling period of 20 months, we see that users of private media are likely to meet more different TPs than users of other types of media. The plots in Figure 12 shows that in some cases, a PSM user will be exposed to as many different TPs as when visiting a private media site.

Discussion and Conclusion

General Presence of TP Services

Expanding on a rights-based approach through the notion of privacy-as-trust that captures not just "notice and choice" consent formats but also what happens to personal data after a user has given consent, this contribution set out to analyze problems relating to PSM institutions' use of TP servers that track, collect, and analyze user behavior. Theoretically, we developed a framework that shows that privacy, as one of the communication rights identified by Nieminen,[60] should be part and parcel of the key values of all legacy media but particularly PSM. As duty-bearers and self-identified islands of trust in a media landscape characterized by

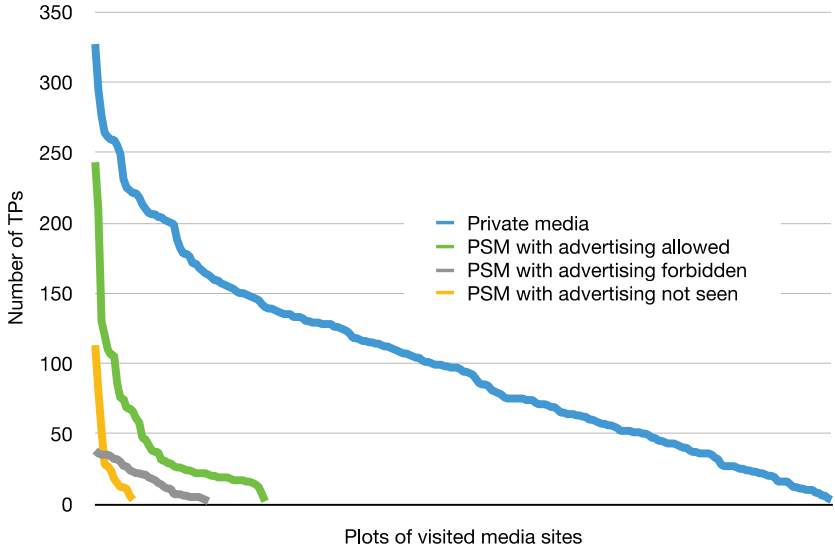

FIGURE 12 Variations in the number of unique TPs for individual media sites, aggregated over 20 months.

60. Nieminen.

datafication and a society driven by surveillance capitalism, PSM institutions have a responsibility toward the rights holder/citizens to deal with their personal data in a way that is not only legal but also ethical. Indeed, based in Waldman's notion of privacy-as trust, we argued that PSM need to think carefully about their core values to incorporate a strong notion of privacy and need to develop policies that respect the rights holders beyond mere consent with terms and agreements. Our empirical analysis of data reflects the presence of a wide range of TPs on websites of private and public service legacy media in Europe, providing much food for thought.

For one, our data confirm that users meet TPs when browsing both private and PSM websites, although the number of different TPs they come across when visiting different media sites varies. To those unfamiliar with technology, the sheer number of TPs found in the sampled (342) websites during our 44 visits is staggering, with 3,511 unique TPs. This wide-spread presence of TPs on European media's websites supports and expands Lindskow's[61] observation for US media that they are highly integrated in a network of TP services. It confirms Moor's[62] late 1990s imaginary of digital data as "greased information," seemingly unstoppable and beyond the grasp not just of the individual but also of the media. As such, our data confirm broad concerns regarding privacy/autonomy—as part of the communication rights—of citizens. These concerns are strengthened by the fact that privacy-related TPs were present at less than half of all sites and that almost one out of three sites had one or more malicious TPs. Concerns for the commodification of these data, too, are confirmed as advertising-related TPs are the biggest group after the category of yet unidentified TPs and the second most present on virtually all sites, after TPs concerned with data analytics category. We see the same pattern for many European media, including many PSM sites. These data certainly confirm that the issue of privacy is part of our media lives more than ever. As Waldman[63] states: "It is a fact of life so engrained in the social structure that we couldn't live without it" (149).

Second, our sampling period started some months before the enforcement of the GDPR, May 25, 2018. Our collection of TP data were initially motivated by a pre-GDPR hypothesis[64] that the number of unique TPs

61. Lindskow.
62. Moor.
63. Waldman.
64. Van den Bulck and Moe.

would decline with the GDPR as this regulation requires data handling agreements between partners that exchange data, in our case media websites and providers of TP webservices that requires exchange of personal data. However, our analysis shows a relatively minor impact of the GDPR and mostly for private media. Further research with different data, for example, qualitative interviews with experts within the advertising industry, can analyze if the decline for private media TPs can be explained by the introduction of the GDPR. Our data suggest, however, that a legal rights approach to privacy such as the GDPR, based in agreement to terms and conditions, does not ensure fair treatment of users' personal data once subjected to trade and algorithms and artificial intelligence. However, following both Waldman and Zuboff, we do not conclude that privacy is "dead" but that it needs to be approached as an issue that starts after consent is given.

Indeed, following Zuboff,[65] we consider that, once involved in the surveillance economy, media, and their users' data are being instrumentalized as any other resource that freely can be exploited to produce value in the surveillance economy. Without any ethical direction or concern about its position as game, it is being subjected to the mechanisms of the surveillance economy. Certainly, the intense integration with TP servers that emerges from our data analysis, suggests that it makes private and PSM institutions dependent on TP providers. This is all the more pressing, given that our data illustrate that TP services increasing become concentrated in a few TP companies, as the top 20 suggests. To give but one example, Google's advertising service *doubleclick.net* was present at almost all Private Media sites, a vast majority of PSM—ads allowed and PSM—no ads seen sites and, even, a number of PSM ads forbidden sites. *Google Analytics* showed a similar dominance. Facebook and Twitter, too, prove a dominant presence across legacy media sites. Consolidation in this regard seems ongoing and will make legacy media further dependent on TP companies that fall outside of the grasp of national and even EU policymakers. As such, the question about who is accountable becomes more pressing: legacy media certainly are duty-bearers in this debate but for their economic survival are dependent on the giant tech companies like Alphabet. As Wagner[66] suggests, though, these big tech companies tend to use the ethical argument as a discursive means to deflect legislative interference from governments

65. Zuboff, "We Make Them Dance."
66. Wagner.

rather than make genuine ethical efforts, confirmed by recent evidence regarding social media giants. Financial repercussions, too, have been shown to be ineffective as even hefty multi-million-dollar fines hardly put a dent in the profit of these giant companies. This puts the burden of duty firmly with legacy media and reinforces the need for an ethical approach of privacy-as-trust.

Tough Choices for PSM as Trusted Institutions

The particular position of PSM in the media landscape, their (partly) public funding in return for a remit based on societal values and their position as "islands of trust" led us to assume that PSM sites would show a different picture from private media sites with regards to the presence of TPs. From a privacy-as-trust perspective, right holders decide on disclosure of personal data based, at least partly, on contextual norms of trust. However, it transpired that presence of TPs did not differ significantly between PSM and private media. Rather the dividing criterion appeared to be the presence of / permission to run advertising as PSM—ads allowed sites showed greater similarities with Private Media sites than with PSM—no ads allowed or PSM—no ads seen. This dominance, particular in PSM that carry advertising, raises several concerns.

For one, all TP companies in the top 20 for PSM—ads allowed sites were also in the top 20 for Private Media sites. The larger numbers of TP servers at pages with advertising relates to the process of selling advertising to advertisers that involves a number of servers, just to find the right bid and buyer for the advertisement.[67] At the time of writing, this ad sales system is being replaced with a system where bidding takes place not in the user's computer, but between the media server and the advertising servers (so-called "server-side header bidding").[68] Furthermore, the European lobby organization for Interactive Advertising, IAB Europe, recently announced we are entering the "Post Third-party cookie Era."[69] As a result, an observed decline in the number of TPs may not necessarily reflect lower exposure of user data but that we cannot measure it any longer. That said, the GDPR seems to have led media and advertising technology companies

67. Acar et al.

68. IAB—Interactive Advertising Bureau Europe, *Header Bidding and Auction Dynamics*.

69. IAB—Interactive advertising bureau Europe. *IAB Europe Guide to the Post Third-Party Cookie Era*.

to clean up unused servers and scripts, thereby reducing some of the exposure of user data. However, the general tendency went in the direction of slowly increasing the use of TPs to deliver content and analyze user behavior.

To the extent that PSM—ads allowed had lower numbers of TPs than Private Media, we argue that this does not necessarily reflect better guarantees in protecting the communication rights of users. Indeed, the question is whether the actual number of TPs is a clear signifier of privacy exposure or whether the presence of a few key players, for example, large TPs such as those of Google and Facebook, already constitute a severe privacy exposure. When we use the term "privacy exposure," we do not consider whether the site is GDPR compliant (that has not been our focus in this contribution) but the ethical viewpoint that the point of departure for the user's interaction with the PSM offerings in the broadcast was non-identifiable. For advertising-free, license-fee, or tax financed PSM services, obviously one cannot argue that users have to pay for the service with their data, as one could argue for private media and social media.

In relationship to our proposition of an ethical approach to privacy and data sharing, the situation for TPs at advertising-free PSM websites is interesting. Are they there because they do not exchange data, because the PSM want to use external services to have a technically more advanced site, or because PSM want a level playing field with private media? Or is the presence of these TPs just an expression of a lack of internal and external policies with regards to the use of TPs?

Privacy-as-Trust, Ethics, and a Rights-Based Approach

Our results illustrate what we consider to be a dilemma for PSM. These media organizations clearly are deeply integrated in international networks when delivering their webpages, interacting with an extensive network of digital business partners that aggregate content, analyze user behavior, sell or buy advertisements, integrate social media, or simply deliver files and scripts. This helps media organizations to optimize editorial work and (where allowed) advertising revenue, and to develop personalized recommendations for its users. It allows PSM to stay up to date regarding the newest technologies, platforms and user interfaces, and to reduce the need to invest in technology. The introduction of GDPR affected the number of these TP services all in all to a limited extent, suggesting that the introduction of such a legal framework does not change the core problem of infringement

of media users privacy/autonomy in a context of their data being exchanged with TPs and being treated through artificial intelligence and algorithms. PSM—and all legacy media—thus find themselves caught up in a dilemma between maintaining their integrity or participating in the exposure/surveillance economy, increasingly managed by international companies.

For PSM, this dilemma crucially is about ethics. With a long tradition as a trusted institution, users may entrust PSM with their data assuming, from Waldman's[70] privacy-as-trust perspective, that "[their] information will be used only in accordance with the norms of trust under which it was shared in the first place" (149). When rights owners repeatedly experience or perceive the duty-bearers to violate that trust, the duty-bearer, that is, PSM, may ultimately lose their position as trusted institution. In that regard, they stand much to lose. This raises important questions for PSM and its policymakers: Can PSM organizations use the same tools as private media and as freely as private media to monitor and optimize attention—tools that operate in the background without the knowledge of the user? Some arguments in favor include the need for PSM to be competitive with commercial media, to maintain relevance for users and to produce value for license-free/public funding. However, as trusted institutions, PSM organizations have an ethical obligation to be trustworthy, that is, honest and transparent in their mode of operation. If nothing else, opaque use of TP servers undermines their very role as "islands of trust," an important legitimation of their funding and existence.

Final Thoughts

Our results suggest that differences between countries do not fit traditional distinctions between national media systems such as those based on political characteristics (as in Hallin and Mancini). It certainly invites us to think about other factors to take into consideration when trying to understand differences between media systems, such as technological advancement. The lack of path dependency in this regard, though, raises questions about how policymakers can have an impact on this beyond legislative instruments. Thinking about TPs from a communication rights approach, focuses on how policymakers can help ensure that the duty-bearers, that is, the digital media can be made to respect the communication rights of the rights holders, that is, the digital media users.

70. Waldman.

Our data are rich and detailed in many aspects. Further and more advanced exploration of the large dataset may reveal more detailed and new patterns compared to the overall findings presented here. Particularly TPs patterns at the level of individual media sites may provide further insights into how media can behave both legally and ethically with regards to communication rights of privacy and information autonomy within a digital media market that necessitates the use of TPs. For instance, a previous study[71] suggests that there are some PSM institutions that minimize the involvement of TP servers at a very low level. More in-depth analysis of such cases potentially can show how higher ethical standards can be maintained without losing the advantages of advanced technological, user friendly design of sites, righting the balance between communication right holders and legacy media, especially PSM, ensuring their continued relevance as trusted institutions.

BIBLIOGRAPHY

Acar, Gunas, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, and Claudia Diaz. "The Web Never Forgets." In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security—CCS '14*, 674–89. New York: ACM Press, 2014. doi:10.1145/2660267.2660347.

Acquisti, Alessandro, Curtis Taylor, and Liad Wagma. "The Economics of Privacy." *Journal of Economic Literature* 54, no. 2 (2016): 442–92.

Ahmed, Iftekhar, Tahmin Nahar, Shahina S. Urmi, and Kazi A. Taher. "Protection of Sensitive Data in Zero Trust Model." Proceedings of the International Conference on Computing Advancements, Dhaka, Bangladesh, 2020, 1–5. doi:10.1145/3377049.3377114.

Allcott, Hunt, and Matthew Gentzkow. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives* 31, no. 2 (2017): 211–36.

Bardoel, Jo, and Leen d'Haenens. "Reinventing Public Service Broadcasting in Europe: Prospects, Promises and Problems." *Media, Culture & Society* 30, no. 3 (2008): 337–55. doi:10.1177/0163443708088791.

Bardoel, Jo, and Gregory F. Lowe. "From Public Service Broadcasting To Public Service Media: The Core Challenge." In *From Public Service Broadcasting To Public Service Media*, edited by Gregory J. Lowe and Jo Bardoel, 9–28. Göteborg: Nordicom, 2007.

Bassett, Laura. "Digital Media Is Suffocating—and It's Facebook and Google's Fault." 2019. Accessed February 2, 2020. https://prospect.org/culture/digital-media-suffocating-and-facebook-google-s-fault/.

Biltereyst, Daniel. "Public Service Broadcasting, Popular Entertainment and the Construction of Trust." *European Journal of Cultural Studies* 7, no. 3 (2004): 341–62. doi:10.1177/1367549404044787.

Born, Georgina, and Tony Prosser. "Culture and Consumerism: Citizenship, Public Service Broadcasting and the BBC's Fair Trading Obligations." *The Modern Law Review* 64, no. 5 (2001): 657–87. doi:10.1111/1468-2230.00345.

71. Sørensen and Van den Bulck.

Busch, Oliver. ed. *Programmatic Advertising*. Cham: Springer International Publishing, 2018. doi:10.1007/978-3-319-25023-6.

Carey, James W. "The Mass Media and Democracy: Between the Modern and the Postmodern." *Journal of International Affairs* 47, no 1 (1993): 1–21.

Chokhani, Santosh. "Trusted Products Evaluation." *Communications of the ACM* 35, no 7 (1992): 64–76. doi:10.1145/129902.129907.

Curran, James. *Media and Democracy*. London: Routledge, 2011.

Denning, Dorothy E. "A New Paradigm for Trusted Systems." *Proceedings on the 1992–1993 Workshop on New Security Paradigms* 129673 (1993): 36–41. doi:10.1145/283751.283772

Dolata, Ulrich. "Apple, Amazon, Google, Facebook, Microsoft: Market Concentration—Competition—Innovation Strategies." In *Stuttgarter Beiträge zur Organisations- und Innovationsforschung, SOI Discussion Paper, No. 2017-01*. Stuttgart: Universität Stuttgart, 2017.

Donders, Karen, Gunn Enli, Tim Raats, and Trine Syertsen. "Digitisation, Internationalisation, and Changing Business Models in Local Media Markets: An Analysis of Commercial Media's Perceptions On Challenges Ahead." *Journal of Media Business Studies* 15, no. 2 (2018): 89–107. doi:10.1080/16522354.2018.1470960.

EBU. "Trust in Media Report 2019." 2017. https://www.ebu.ch/news/2019/05/trust-gap-between-traditional-and-new-media-grows.

EBU Digital Strategy Group. *Media with a Purpose: Public Service Broadcasting in the Digital Age*. Geneva: EBU, 2002. https://www.ebu.ch/CMSimages/en/DSG_final_report_E_tcm6-5090.pdf.

EBU Media Intelligence Service. *Market Insights: Trust in Media 2016–2017*. Geneva: EBU, 2017.

Englehardt, Steven, and Arvind Narayanan. "Online Tracking: A 1-million-site Measurement and Analysis." CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, October 2016, 1388–14011. doi:10.1145/2976749.2978313.

EU Parliament. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)." 2002. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

European Commission. *The EU Internet Handbook, Cookies*. Brussels: European Commission, 2016. http://ec.europa.eu/ipg/basics/legal/cookies/index_en.html.

Falahrastegar, Marjan, Hamed Haddadi, Steve Uhlig, and Richard Mortier. "Anatomy of the Third-Party Web Tracking Ecosystem." 2014. http://arxiv.org/abs/1409.1066.

Gilman, Evan, and Doug Barth. *Zero Trust Networks*. Boston: O'Reilly Media, 2017.

Hallin, David, and Paolo Mancini. *Comparing Media Systems: Three Models of Media and Politics*. Cambridge: Cambridge University Press, 2004.

Hanitzsch, Thomas, Arjen Van Dalen, and Nina Steindl. "Caught in the Nexus: A Comparative and Longitudinal Analysis of Public Trust in the Press." *The International Journal of Press/Politics* 23, no. 1 (2018): 3–23.

IAB—Interactive Advertising Bureau Europe. "Header Bidding and Auction Dynamics." 2018. https://www.iab.it/wp-content/uploads/2018/09/IAB-Europe_Header-Bidding-and-Auction-Dynamics-White-Paper_August-2018-1-compressed.pdf.

———. "IAB Europe Guide to the Post Third-Party Cookie Era." 2020. Accessed August 4, 2020. https://iabeurope.eu/knowledge-hub/iab-europe-guide-to-the-post-third-party-cookie-era/.

Internet Engineering Task Force. "RFC 6265: HTTP State Management Mechanism ('HTTP cookie')." 2011. Accessed November 2, 2017. https://tools.ietf.org/html/rfc6265.

Jones, Jeffrey M. "U.S. Media Trust Continues To Recover From 2016 Low." *Gallup*, October 12, 2018. https://news.gallup.com/poll/243665/media-trust-continues-recover-2016-low.aspx.

Just, Natascha, and Michael Latzer, "Governance By Algorithms: Reality Construction By Algorithmic Selection On the Internet." *Media, Culture and Society* 39, no. 2 (2017): 238–58. doi:10.1177/0163443716643157.

Kirkemann Boesen, Jakob, and Tomas Martin. *Applying a Rights-Based Approach: An Inspiration Guide for Civil Society*. Copenhagen: Danish Institute for Human Rights, 2007.

Lindskow, Kasper. *Exploring Digital News Publishing Business Models—A Production Network Approach*. Copenhagen: Copenhagen Business School, 2016. http://hdl.handle.net/10398/9284.

Mayer, Roger C., James H. Davis, and F. David Schoorman. "An Integrative Model of Organizational Trust." *Academy of Management Review* 20, no. 3 (1995): 713. doi:10.1145/129902.129907.

Mayer-Schoenberger, Viktor, and Kenneth Cukier. *Big Data. A Revolution That Will Transform How We Live, Work, and Think*. London: John Murray Publishers, 2013.

McChesney, Robert W., and John Nichols. *The Death and Life of American Journalism: The Media Revolution that Will Begin the World Again*. New York: Nation Books, 2010.

Moor, James H. "Towards a Theory of Privacy in the Information Age." *ACM SIGCAS Computers and Society* 27 no. 3 (1997): 27–32. doi:10.1145/270858.270866

Newman, Nic, Richard Fletcher, Antonis Kalogeropoulos, David A. L. Levy, and Rasmus Kleis Nielsen. *Reuters Institute Digital News Report 2017. Technical Report*. Oxford: Reuters Institute for the Study of Journalism, 2017. Available at SSRN: https://ssrn.com/abstract=3026082.

Nieminen, Hannu. "Why Study Media Policy and Regulation." In *Comparative Media Policy, Regulation and Convergence in Europa*, edited by Leen d'Haenens, Helena Sousa, and Josef Trappel. Bristol: Intellect, 2018.

Nyamu-Musembi, Celestine, and Andrea Cornwall. *What is the 'Rights-Based Approach' All About? Perspectives from International Development Agencies. IDS Working Paper 234*. Brighton: Institute of Development, 2004. https://www.ids.ac.uk/files/dmfile/Wp234.pdf.

Patel, Nilay. "Facebook's $5M FTC is an Embarrassing Joke: Facebook Gets Away with it again." *The Verge*, July 12, 2019. https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke.

Raats, Tim, Tom Evens, and Caroline Pauwels. "Towards Sustainable Financing Models for Television Production? Challenges for Audiovisual Policy Support in Small Media Markets." Proceedings of the 30th European Communications Policy Research Conference (EuroCPR), Brussels, Belgium, March 23–24, 2015.

Roesner, Franziska, Tadayoshi Kohno, and David Wetherall. "Detecting and Defending against Third-party Tracking on the Web." Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation (NSDI'12, 2020), Santa Clara, CA, 2020.

Sjøvaag, Helle, Eirik Stavelin, Michael Karlsson, and Aske Kammer. "The Hyperlinked Scandinavian News Ecology. The Unequal Terms Forged By the Structural Properties of Digitalisation." *Digital Journalism* 7, no. 4 (2019): 507–31.

Sørensen, Jannick and Sokol Kosta, "Before and After GDPR: The Changes in Third Party Presence at Public and Private European Websites," *The World Wide Web Conference* (WWW '19). Association for Computing Machinery (New York, 2019): 1590–1600. DOI:10.1145/3308558.3313524

Sørensen, Jannick K. and Hilde Van den Bulck, "Public Service Media Online, Advertising and the Third-Party User Data Business: A Trade versus Trust Dilemma?" *Convergence, The International Journal of Research into New Media Technologies* 26, no 2 (2020): 421–447.

Srnicek, Nick. *Platform Capitalism*. London: Wiley, 2017.

Stoll, Julia. "Trust in Media in Europe: Statistics and Facts." *Statista*, March 18, 2019. https://www.statista.com/topics/3303/trust-in-media-in-europe/.

Syvertsen, Trine, Karen Donders, Gunn Enli, and Tim Raats. "Media Disruption and the Public Interest: How Private Media Managers Talk About Responsibility To Society In an Era of Turmoil." *Nordic Journal of Media Studies* 1 (2019): 11–28. doi:10.2478/njms-2019-0002.

Tao, Yang, Zhu Lei, and Peng Ruxiang. "Fine-Grained Big Data Security Method Based on Zero Trust Model." IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS, 2018), 2018, 1040–45. doi:10.1109/PADSW.2018.8644614.

Tsfati, Yarif, and Gal Ariely. "Individual and Contextual Correlates of Trust in Media Across 44 Countries." *Communication Research* 20, no. 10 (2013): 1–23. doi:10.1177/0093650213485972.

Urban, Tobias, Dennis Tatang, Martin Degeling, Thorston Holz, and Norbert Pohlmann. "The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR." 2018. http://arxiv.org/abs/1811.08660.

———. "Measuring the Impact of the GDPR on Data Sharing in Ad Networks." Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20), ASIA CCS, Taipei, Taiwan, June 1–5, 2020. doi:10.1145/3320269.3372194.

Urban, Tobias, Dennis Tatang, Thorston Holz, and Norbert Pohlmann. "Towards Understanding Privacy Implications of Adware and Potentially Unwanted Programs." In *Computer Security*, edited by Javier Lopez, Jianying Zhou, and Miguel Soriano, 449–69 Cham: Springer International Publishing, 2018. doi:10.1007/978-3-319-99073-6_22.

Vaidhyanathan, Siva. *Anti-Social Media: How Facebook Disconnects Us and Undermines Democracy*. Oxford: Oxford University Press, 2018.

Van den Bulck, Hilde. "Public Service Broadcasting and National Identity as a Project of Modernity," *Media, Culture and Society* 23, no. 1 (2001): 53–69. doi: 10.1177/016344301023001003

Van den Bulck, Hilde, Karen Donders and Greg F. Lowe. "Public Service Media In the Networked Society: What Society? What Network? What Role?" *Public Service Media In the Networked Society* (pp. 11–28), edited by Greg F Lowe, Hilde Van den Bulck, and Karen Donders, Gothenburg: NORDICOM, 2018.

Van den Bulck, Hilde and Hallvard Moe. "Universality and Personalisation Through Algorithms: Mapping Strategies and Exploring Dilemmas," *Media Culture and Society* 40, no. 6 (2018): 875–892.

Van Dijck, Jose. "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology." *Surveillance and Society* 12, no. 2 (2014). doi:10.24908/ss.v12i2.4776.

Wagner, Ben. "Ethics As an Escape from Regulation: From Ethics-Washing to Ethics-Shopping?" *Being Profiling. Cogitas ergo sum*, edited by Mireille Hildebrandt. Amsterdam: Amsterdam University Press, 2018.

Waldman, Ari Ezra. *Privacy as Trust: Information Privacy for an Information Age*. Cambridge: Cambridge University Press, 2018.

Wambach, Tim, and Katharina Bräunlich. "The Evolution of Third-Party Web Tracking." In *Information Systems Security and Privacy. ICISSP 2016. Communications in Computer and Information Science*, 130–47. Cham, Switzerland: Springer, 2017. doi:10.1007/978-3-319-54433-5_8.

Yan, Zheng. "A Comprehensive Trust Model for Component Software." Proceedings of the 4th International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Sorrento, Italy, 2008, 1–6. doi:10.1145/1387329.1387330.

Zuboff, Shoshana. "'We Make Them Dance': Surveillance Capitalism, the Rise of Instrumentarian Power, and the Threat to Human Rights." *Human Rights in the Age of Platforms*, edited by R. F. Jørgensen and D. Kaye, 3–51. Cambridge, MA: MIT Press, 2019a.

———. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs, 2019b.